

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

DISH NETWORK LLC et al.,

Plaintiffs,

vs.

ANDREW DIMARCO et al.,

Defendants.

2:11-cv-01962-RCJ-PAL

ORDER

This case arises out of the alleged sale of devices designed to illegally circumvent Plaintiffs' communications security system in order to intercept copyrighted, subscription-based satellite programming. The Court previously granted Plaintiffs a preliminary injunction because Defendants did not respond to the motion, answer the Complaint, or otherwise appear before the deadlines to respond to the motion or to answer the Complaint passed. The Court granted Defendants' motion to set aside the preliminary injunction based upon evidence of counsels' discussions concerning an extension to respond and answer. Defendants have now answered the Complaint and responded to the original motion for preliminary injunction, which is now before the Court. For the reasons given herein, the Court grants the motion in part and denies it in part.

I. FACTS AND PROCEDURAL HISTORY

Plaintiff Dish Network LLC is a multi-channel video provider that delivers audio, video, and data services to customers throughout the United States via satellite for subscription or pay-per-view fees. (*See* Compl. ¶¶ 12–13, Dec. 7, 2011, ECF No. 1). Dish Network has the authority of the owners of the copyrighted works it broadcasts to protect those works from unauthorized

1 reception and viewing. (*Id.* ¶¶ 14–15). In order to ensure that only subscribers can receive its
2 broadcasts, Dish Network electronically digitizes, compresses, and scrambles its programming
3 prior to transmitting it to multiple communications satellites in geosynchronous orbit above
4 North America, which satellites relay the broadcasts to subscribers throughout North America
5 who may view the programming using Dish Network’s decoding equipment. (*Id.* ¶ 16). Plaintiff
6 EchoStar Technologies LLC (“EchoStar”) provides receivers, satellite antennae, and other
7 digital equipment to Dish Network for its customers’ use, and Plaintiff NagraStar LLC provides
8 “smart cards” and other security equipment. (*Id.* ¶ 17).

9 When an EchoStar receiver receives a Dish Network signal, it forwards part of the signal
10 called the “entitlement control message” to the NagraStar smart card. (*Id.* ¶ 21). If the subscriber
11 is tuned to a channel he is authorized to receive, the smart card retrieves a decryption key from
12 its read-only memory and uses the key to unlock the “control word” from the entitlement control
13 message. (*Id.* ¶¶ 20–21). The smart card then transmits the control word back to the receiver,
14 and the receiver uses it to decode the incoming signal so the subscriber can watch the
15 programming. (*Id.* ¶¶ 21–22). Each EchoStar receiver and NagraStar smart card receives a
16 unique serial number when activated to ensure that a subscriber may decode only the
17 programming that he has paid Dish Network to receive. (*Id.* ¶ 18).

18 Various devices designed to illegally decrypt satellite signals from service providers such
19 as Dish Network can be purchased on the black market. (*Id.* ¶ 23). One method used to
20 circumvent Dish Network’s communications security systems is called a “free-to-air” or “FTA”
21 system. (*Id.* ¶ 24). The FTA method of piracy was initially accomplished by loading software
22 with proprietary data and decryption keys onto unauthorized receivers in order to mimic a
23 legitimate NagraStar smart card, a process called “flashing” a receiver. (*Id.* ¶¶ 24–25). Piracy
24 software is available for free on the Internet for this purpose. (*Id.* ¶ 25). A service provider such
25 as Dish Network can counteract this practice by routinely changing its decryption keys, but a

1 new form of piracy has arisen called “Internet key sharing” or “IKS” whereby a pirate keeps his
2 unauthorized receiver connected to the Internet for automatic re-flashing with the newest keys,
3 which are retrieved from an IKS server connected to multiple legitimate NagraStar smart cards.
4 (*See id.* ¶¶ 26–28).

5 Defendants offer unauthorized receivers with decryption software and hardware, e.g.,
6 Sonicview and Limesat brand receivers, to the public, through their websites
7 (<www.coolsatellite.com> and <www.satmonster.com>) and otherwise. (*Id.* ¶¶ 30–33).
8 Defendants also offer cables to connect unauthorized receivers to the Internet for use of an IKS
9 server, as well as passwords to access the IKS server, which passwords Defendants refer to using
10 the euphemism “extended warranty codes.” (*Id.* ¶¶ 34–36). Defendants advertise their products
11 on piracy-related websites such as <www.myfreeneeds.com>. (*Id.* ¶ 38). Defendants also direct
12 their own customers to that website for piracy-related support, both via a direct link on their own
13 website and during live online chat sessions. (*Id.*).

14 Plaintiffs sued Defendants Andrew Dimarco, David Dimarco, and Digital Warehouse,
15 Inc. in this Court on five causes of action: (1) Sale and Trafficking of Circumvention Devices
16 and Services in violation of the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C.
17 § 1201(a)(2); (2) Distribution of Signal Theft Devices in violation of the Communications Act,
18 47 U.S.C. § 605(e)(4); (3) Circumvention of Access Control Measures in violation of DMCA, 17
19 U.S.C. § 1201(a)(1); (4) Receipt and Assisting Others in Receipt of Satellite Signals Without
20 Authorization in violation of the Communications Act, 47 U.S.C. § 605(a); and (5) Interception
21 of and Procurement of Others to Intercept Satellite Signals in violation of the Electronic
22 Communications Privacy Act (“ECPA”), 18 U.S.C. §§ 2511(a)(1) and 2520. Plaintiffs moved
23 for a preliminary injunction. Because no Defendant had timely responded, answered the
24 Complaint, or otherwise appeared, the Court granted the motion and signed Plaintiffs’ proposed
25 preliminary injunction order. Defendants then made their first appearance via an emergency

1 motion to set aside the preliminary injunction order. The Court granted that motion based upon
2 evidence that Plaintiffs' counsel had discussed an extension to respond with Defendants'
3 counsel. Before the Court are the merits of the original preliminary injunction motion, to which
4 Defendants have now substantively responded.

5 **II. LEGAL STANDARDS**

6 Under Fed. R. Civ. P. 65(b), a plaintiff must make a showing that immediate and
7 irreparable injury, loss, or damage will result to plaintiff without a temporary restraining order.
8 Temporary restraining orders are governed by the same standard applicable to preliminary
9 injunctions. *See Cal. Indep. Sys. Operator Corp. v. Reliant Energy Servs., Inc.*, 181 F. Supp. 2d
10 1111, 1126 (E.D. Cal. 2001) ("The standard for issuing a preliminary injunction is the same as
11 the standard for issuing a temporary restraining order."). The standard for obtaining *ex parte*
12 relief under Rule 65 is very stringent. *Reno Air Racing Ass'n v. McCord*, 452 F.3d 1126, 1130
13 (9th Cir. 2006). The temporary restraining order "should be restricted to serving [its] underlying
14 purpose of preserving the status quo and preventing irreparable harm just so long as is necessary
15 to hold a hearing, and no longer." *Granny Goose Foods, Inc. v. Bhd. of Teamsters & Auto Truck*
16 *Drivers Local No. 70*, 415 U.S. 423, 439 (1974).

17 The Ninth Circuit in the past set forth two separate sets of criteria for determining
18 whether to grant preliminary injunctive relief:

19 Under the traditional test, a plaintiff must show: (1) a strong likelihood of success
20 on the merits, (2) the possibility of irreparable injury to plaintiff if preliminary
21 relief is not granted, (3) a balance of hardships favoring the plaintiff, and (4)
22 advancement of the public interest (in certain cases). The alternative test requires
that a plaintiff demonstrate either a combination of probable success on the merits
and the possibility of irreparable injury or that serious questions are raised and the
balance of hardships tips sharply in his favor.

23 *Taylor v. Westly*, 488 F.3d 1197, 1200 (9th Cir. 2007). "These two formulations represent two
24 points on a sliding scale in which the required degree of irreparable harm increases as the
25 probability of success decreases." *Id.*

1 The Supreme Court recently reiterated, however, that a plaintiff seeking an injunction
2 must demonstrate that irreparable harm is “likely,” not just possible. *Winter v. NRDC*, 129 S. Ct.
3 365, 374–76 (2008) (rejecting the Ninth Circuit’s alternative “sliding scale” test). The Ninth
4 Circuit has explicitly recognized that its “possibility” test was “definitively refuted” in *Winter*,
5 and that “[t]he proper legal standard for preliminary injunctive relief requires a party to
6 demonstrate ‘that he is likely to succeed on the merits, that he is likely to suffer irreparable harm
7 in the absence of preliminary relief, that the balance of equities tips in his favor, and that an
8 injunction is in the public interest.’” *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1127 (9th Cir.
9 2009) (quoting *Winter*, 129 S. Ct. at 374) (reversing a district court’s use of the Ninth Circuit’s
10 pre-*Winter*, “sliding-scale” standard and remanding for application of the proper standard).

11 A recent Ninth Circuit ruling relying largely on the dissenting opinion in *Winter* parsed
12 the language of *Winter* and subsequent Ninth Circuit rulings and determined that the sliding
13 scale test remains viable when there is a lesser showing of likelihood of success on the merits
14 amounting to “serious questions,” but not when there is a lesser showing of likelihood of
15 irreparable harm. See *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1134 (9th Cir.
16 2011). This case presents some difficulty in light of *Winter* and prior Ninth Circuit cases. To
17 the extent *Cottrell*’s interpretation of *Winter* is inconsistent with *Selecky*, *Selecky* controls. *Miller*
18 *v. Gammie*, 335 F.3d 889, 899 (9th Cir. 2003) (en banc) (holding that, in the absence of an
19 intervening Supreme Court decision, only the en banc court may overrule a decision by a
20 three-judge panel). In any case, the Supreme Court stated in *Winter* that “[a] plaintiff seeking a
21 preliminary injunction must establish that he is *likely* to succeed on the merits, that he is *likely* to
22 suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his
23 favor, *and* that an injunction is in the public interest.” *Winter*, 129 S. Ct. at 374 (citing *Munaf v.*
24 *Geren*, 128 S. Ct. 2207, 2218–19 (2008); *Amoco Prod. Co. v. Gambell*, 480 U.S. 531, 542
25 (1987); *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 311–12 (1982)) (emphases added). The

1 test is presented as a four-part conjunctive test, not as a four-factor balancing test, and the word
2 “likely” modifies the success-on-the-merits prong in exactly the same way it separately modifies
3 the irreparable-harm prong. In rejecting the sliding-scale test, the *Winter* Court emphasized the
4 fact that the word “likely” modifies the irreparable-injury prong. *See id.* at 375. The word
5 “likely” also modifies the success-on-the-merits prong. *See id.* at 374.

6 In summary, to satisfy *Winter*, a movant must show that he is “likely” to succeed on the
7 merits. “Likely” means “having a high probability of occurring or being true.”
8 Merriam–Webster Dictionary, <http://www.merriam-webster.com/dictionary/likely>. This
9 colloquial, lay definition of “likely” seems too stringent. Though it could be read consistently
10 with the *Winter* language, Merriam–Webster’s definition of “likely” would appear to require a
11 showing corresponding to the clear-and-convincing evidence standard, because something with a
12 “high probability” of being true has more than a mere greater-than-not chance of being true.
13 Black’s Law Dictionary, a more contextual reference work, defines the “likelihood-of-success-
14 on-the-merits test” more leniently as “[t]he rule that a litigant who seeks [preliminary relief]
15 must show a reasonable probability of success” *Black’s Law Dictionary* 1012 (9th ed.
16 2009). The Court must reconcile the cases by interpreting the *Cottrell* “serious questions”
17 requirement to be in harmony with the *Winter/Selecky* “likelihood” standard, not as being in
18 competition with it. “Serious questions going to the merits” must mean that there is at least a
19 reasonable probability of success on the merits. On its face, “serious questions” appears to focus
20 on the gravity of the issues but appears silent on the probability of the truth of the proffered
21 proposition, which is the focus of the success-on-the-merits prong. The gravity of the issues is
22 separately considered under the balance-of-hardships prong. The *Cottrell* Court must have
23 meant something like “reasonable probability,” which appears to be the most lenient position on
24 the sliding scale that can satisfy the requirement that success on the merits be “likely.” If
25 success on the merits is merely possible, but not reasonably probable, no set of circumstances

1 with respect to the other prongs will justify preliminary relief.

2 **III. ANALYSIS**

3 Defendants admit that they sell the products alleged, i.e., receivers capable of being used
4 for the piracy Plaintiffs describe, but argue that because they do not themselves illegally traffic
5 encryption keys, their products amount to “modern-day rabbit ears” for their customers to
6 receive free satellite programming. Defendants note that its Sonicview receivers have no built-in
7 means of connecting to the Internet. Defendants previously sold adapters for this purpose but
8 ceased doing so at the request of Plaintiffs before the present lawsuit was filed. They have also
9 agreed to stop selling their “extended warranty codes,” which Plaintiffs argue simply consist of
10 passwords to Internet sites used to access pirated decryption keys via an IKS server. Defendants
11 do not directly address whether this is indeed the nature of the “extended warranty codes” they
12 previously sold. Defendants argue that they no longer sell any items to connect its receivers to
13 the Internet, and that they are not liable for their customers’ misuse of their products, which have
14 legitimate uses.

15 One disputed product that Defendants have agreed to stop selling is called the WizHub,
16 which is a device used to connect a receiver to the Internet. Defendants argue that the Court
17 should not grant a preliminary injunction to impound its WizHubs or its extended warranty
18 codes, because the WizHub is simply an adapter, and one cannot engage in piracy without the
19 piracy software and IKS servers. Section 1201 of the DMCA states, “No person shall circumvent
20 a technological measure that effectively controls access to a work protected under this title.” 17
21 U.S.C. § 1201(a)(1). The statute also prohibits trafficking in devices that are “primarily
22 designed or produced for the purpose of circumventing a technological measure that effectively
23 controls access to a work protected under this title,” *id.* § 1201(a)(2)(A), that have “only limited
24 commercially significant purpose or use other than to circumvent a technological measure that
25 effectively controls access to a work protected under this title,” *id.* § 1201(a)(2)(B), or which “is

1 marketed by that person or another acting in concert with that person with that person's
2 knowledge for use in circumventing a technological measure that effectively controls access to a
3 work protected under this title," *id.* § 1201(a)(2)(C). In other words, Defendants' products need
4 have been primarily designed for piracy, need have only a limited commercially significant non-
5 piracy purpose, or need have been marketed by Defendants for the purpose of piracy. Plaintiffs
6 have a reasonable probability of succeeding on the claim that the WizHub and the "extended
7 warranty codes" fit one or all of these prongs. A device such as the WizHub permitting the
8 connection of an otherwise legitimate receiver to the Internet along with a password permitting
9 access to a server with illegally trafficked decryption keys can be said to constitute a product
10 designed to circumvent a technological measure that effectively controls access to a protected
11 work. Impoundment of such devices is a permitted remedy. *See id.* § 1203(b)(2).

12 Defendants argue that neither the WizHub nor the "extended warranty codes" violate the
13 statute by "circumvent[ing] a technological measure" because they do not "descramble a
14 scrambled work, . . . decrypt an encrypted work, or otherwise . . . avoid, bypass, remove,
15 deactivate, or impair a technological measure, without the authority of the copyright owner." *See*
16 *id.* § 1203(a)(3)(A). The Court rejects this interpretation of the statute. The WizHub connector
17 and passwords to the IKS server are almost certainly designed to "otherwise avoid, bypass, etc."
18 effective technological security measures. Plaintiffs note that the legitimate uses of the receivers
19 they sell is to receive free satellite signals, i.e., open-air signals from artificial satellites
20 analogous to open-air signals from traditional land-based television transmission towers. This
21 would appear to be a legitimate use. But what possible need does a person using a free-to-air
22 satellite receiver in a legitimate way have to connect that receiver to the Internet and enter a
23 password to connect to a server whose sole purpose is the trafficking of decryption keys? The
24 WizHub and "extended warranty codes" therefore are legitimate targets of an impound order.
25 According to their uses as described by both Plaintiffs and Defendants, these appear to be the

1 kinds of devices Congress was targeting via the DMCA. Defendants also make a slippery slope
2 argument that if the WizHub is subject to impoundment, then so is any television or computer
3 used to view pirated programming, any equipment of an internet service provider whose
4 customers use its services for piracy, the equipment of any credit card company that allows its
5 customers to purchase the WizHub, etc. Defendants ignore the statutory requirement that subject
6 devices be designed for piracy, have no significant non-piratical commercial use, or be sold for
7 the purpose of piracy, none of which apply generally to televisions, computers, internet service
8 providers, or credit cards. Defendants themselves note that Plaintiffs do not even seek to have
9 the free-to-air receivers themselves impounded. Presumably, Plaintiffs recognize that those
10 receivers, like televisions and credit cards, are not the proper targets of impoundment under the
11 DMCA. Defendants call the absence of any claim by Plaintiffs that the receivers themselves
12 should be impounded “curious,” particularly as Plaintiffs refer to the receivers as
13 “unauthorized.” Plaintiffs’ use of the phrase “unauthorized receivers” to describe Defendants’
14 receivers generally is perhaps sloppy rhetoric, but Plaintiffs’ failure to request their
15 impoundment along with the WizHubs and extended warranty codes tends to show that Plaintiffs
16 in fact recognize the proper limits of the statute’s application.

17 Defendants next argue that their websites should not be seized. The DMCA permits a
18 court to “grant temporary and permanent injunctions on such terms as it deems reasonable to
19 prevent or restrain a violation.” *See id.* § 1203(b)(1). Defendants argue that because the WizHub
20 and extended warranty codes do not violate the DMCA, seizure of the websites on which they
21 are sold is inappropriate. The Court finds that impoundment of the WizHub devices and the
22 extended warranty codes is appropriate; however, once this impoundment is complete, there
23 seems to be no further reason to seize the websites if there are no further violative uses. The
24 Court will not seize the websites, which appear to be used for the legitimate sale of free-to-air
25 receivers. Plaintiffs will remain free to reinstate this request if Defendants display intransigence

1 by renewing the sale of violative devices on these websites in the future.

2 Defendants argue that their assets should not be frozen. Plaintiffs argue that freezing
3 Defendants' assets is necessary to prevent their use in further piracy-related activity. The Court
4 will not freeze Defendants' assets as a general matter based upon this speculation. It appears
5 that the business consists at least in part in selling legitimate satellite receivers, and those
6 violative devices that Defendants possess will be impounded. Plaintiffs will remain free to
7 reinstate this request if Defendants are seen to engage in further violative activities during the
8 present case.

9 In summary, Plaintiffs are likely to succeed on their DMCA claims that Defendants'
10 trafficking in the WizHub devices and extended warranty codes violate the statute. Plaintiffs
11 will be irreparably harmed through the loss of subscription fees they would otherwise receive by
12 potential customers who receive encrypted, subscription-based programming for free via those
13 devices. The balance of hardships weighs in favor of Plaintiffs. Plaintiffs are correct that the
14 loss of profits gained through activity that has been shown likely to violate a statute "merits little
15 equitable consideration." *See Cadence Design Sys., Inc. v. Avant! Corp.*, 125 F.3d 824, 830 (9th
16 Cir. 1997). Finally, the public interest weighs in favor of preventing piracy.

17 ///

18 ///

19 ///

20 ///

21 ///

22 ///

23 ///

24 ///

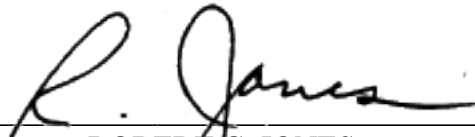
25 ///

CONCLUSION

IT IS HEREBY ORDERED that the Motion for Preliminary Injunction (ECF No. 7) is GRANTED in part and DENIED in part. The WizHub devices and extended warranty codes shall be impounded, but Defendants' websites shall not be seized and their assets shall not be frozen at this time.

IT IS SO ORDERED.

Dated this 13th day of March, 2012.



ROBERT C. JONES
United States District Judge